Von der Enigma zum elektronischen Personalausweis

Die Mathematik der Kryptographie

Ulrich Görtz

Science Pub Stuttgart, 14.3.2016

UNIVERSITÄT DUISBURG ESSEN

Essener Seminar für Algebraische Geometrie und Arithmetik

Science Pub Quiz

Frage

Welcher Wochentag ist in 699 *Tagen?*

(A) Samstag

(B) Sonntag (B) Sonntag

(C) Montag

(D) Dienstag

Science Pub Quiz

Frage

Wie lange dauert es, auf einem handelsüblichen Computer eine Primzahl mit 1200 *Stellen zu finden?*

(A) einige Mikrosekunden

(B) einige Sekunden

(C) einige Minuten

(D) einige Stunden

Quiz Grundfrage der Kryptographie Schlüsseltausch Rechnen mit Resten

Science Pub Quiz

Frage

Wie lange dauert es in ungünstigen Fällen, auf einem handelsüblichen Computer die Primfaktorzerlegung einer Zahl mit 500 Stellen zu finden?

(A) einige Stunden

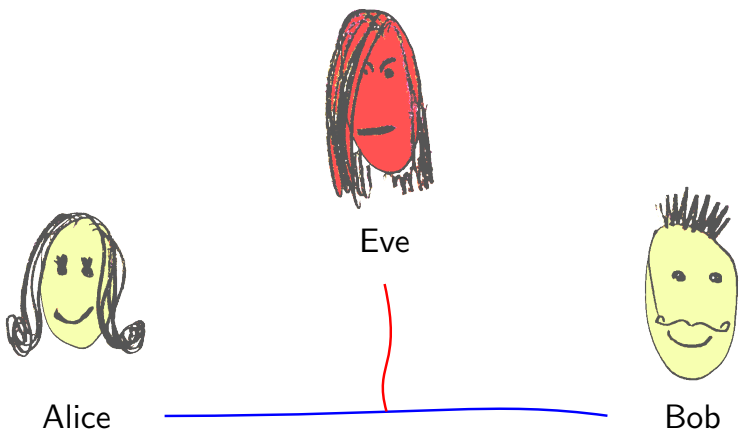
(B) einige Tage

(C) einige Jahre

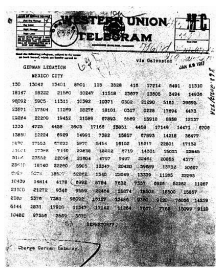
(D) einige Tausend Jahre

Grundlegendes Ziel

Übermittle eine Nachricht so, dass ein Außenstehender sie nicht entschlüsseln kann.

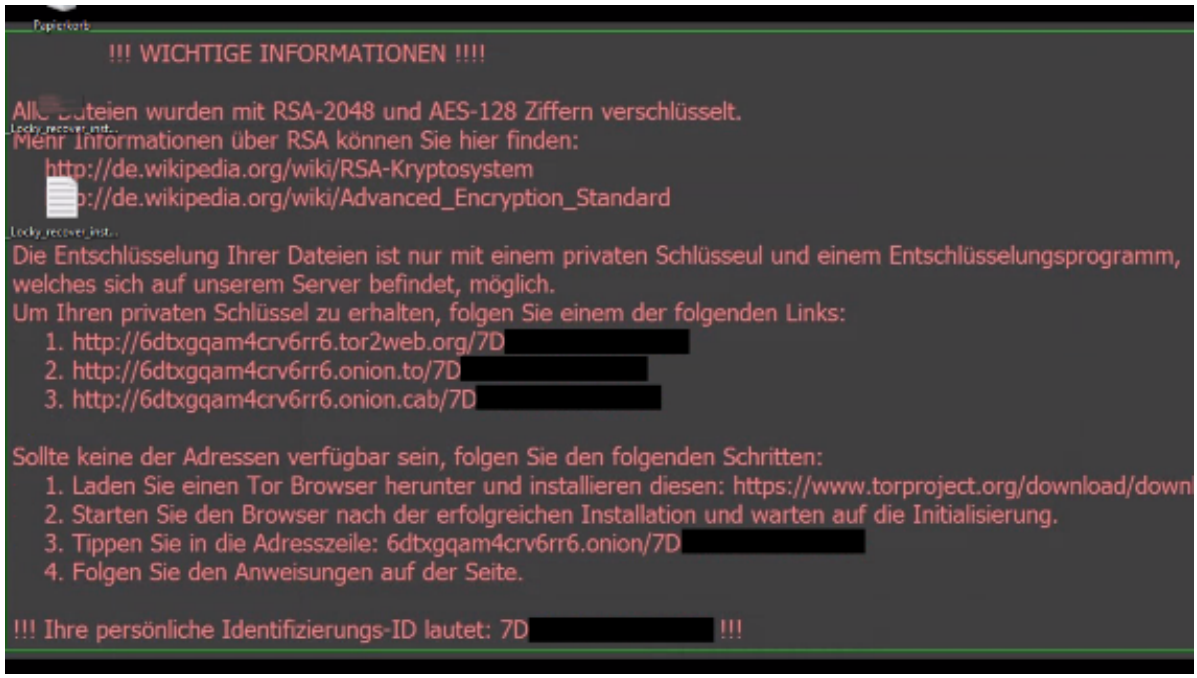


Quiz Grundfrage der Kryptographie Schlüsseltausch Rechnen mit Resten



Bilder: Wikipedia. Zimmermann-Telegramm: Gemeinfrei; Enigma: CC BY-SA Benutzer: JochenF u.a.; Personalausweis: Gemeinfrei.

Locky



Monoalphabetische Verschlüsselung: Jeder Buchstabe wird durch einen anderen Buchstaben ersetzt, und zwar immer durch denselben.

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	...
F	*R*	*Z*	*E*	*G*	*A*	*U*	*B*	*C*	*K*	*O*	*S*	*D*	*X*	*I*	...

Leicht zu knacken durch “Häufigkeitsanalyse”.

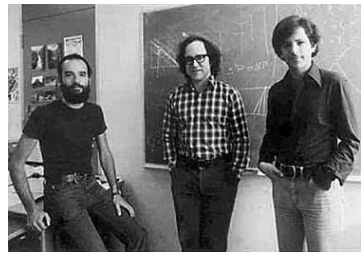
Moderne Verfahren (computerbasiert): DES, AES. Dazu wird ein gemeinsamer “Schlüssel” vereinbart.

Public-Key-Kryptographie

Seit Mitte der 1970er Jahre wurden mehrere Verfahren erfunden, bei denen kein vorheriger Schlüsseltausch notwendig ist.

W. Diffie

M. Hellman



R. Rivest, A. Shamir, L. Adleman

Bilder 1, 2: Wikipedia. Whitfield Diffie: CC-BY, W. Diffie/SUN; Martin Hellman: CC BY-SA M. Hellman;

3: `http://www.ams.org/samplings/feature-column/fcarc-internet`

Grundprinzip: Mathematische Einbahnstraßen

Es gibt mathematische Rechnungen, die leicht durchzuführen, aber schwer umzukehren sind:

Sind p_1, p_2 große Primzahlen, so lässt sich das Produkt $N = p_1 p_2$ leicht berechnen ("schriftliche Multiplikation").

Ist nur n bekannt, so sind die Primfaktoren p_1 und p_2 bestimmt ("eindeutige Primfaktorzerlegung"), aber in der Regel nicht leicht zu finden.

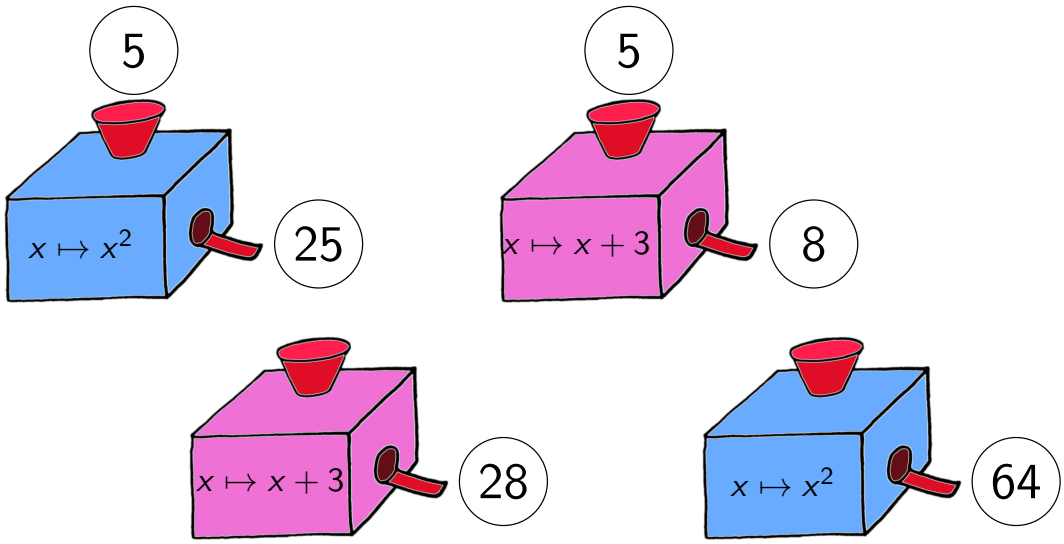
Beispiel

$$257 \cdot 379 = 97403$$

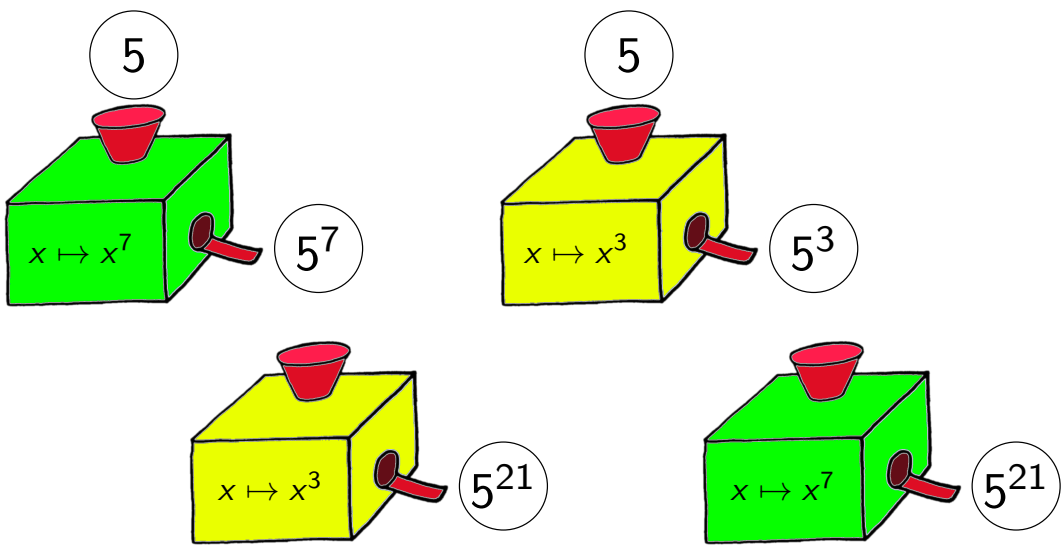
Beispiel

$$95567 = 227 \cdot 421$$

Vertauschbare Maschinen



Vertauschbare Maschinen



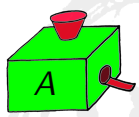
Diffie-Hellman-Schlüsseltausch

Öffentliche Daten: x, die "Bauart" der Maschinen.

Quiz Grundfrage der Kryptographie Schlüsseltausch Rechnen mit Resten

Diffie-Hellman-Schlüsseltausch

Alice



x, $B(x)$, $A(B(x))$,

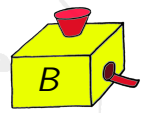
$A(B(x))$

berechne + übermittle $A(x)$

berechne $A(B(x))$

Bob

x x, $A(x)$ x, $A(x)$, $B(A(x))$ x,



$A(x)$, $B(A(x))$

berechne + übermittle $B(x)$

berechne $B(A(x))$

Eve: x, $A(x)$, $B(x)$: x, $A(x)$, $B(x)$

Diffie-Hellman-Schlüsseltausch

Ergebnis:

Alice kennt $A(B(x))$, Bob kennt $B(A(x))$,

Eve kennt x, $A(x)$, $B(x)$.

- Falls $A(B(x)) = B(A(x))$, so kann dieser Wert nun als Schlüssel benutzt werden.
- Sicherheit: Es darf nicht (leicht) möglich sein, aus x, $A(x)$ und $B(x)$ auf A oder B (und damit $A(B(x))$) zurückzuschließen.

Erster Versuch ...

Sei x eine Zahl, zum Beispiel $x = 5$.

Alice wählt eine Zahl A, zum Beispiel $A = 3$ und benutzt als $A(x)$ den Wert $x^A = 5^3$.

Bob wählt eine Zahl B, zum Beispiel $B = 7$ und benutzt als $B(x)$ den Wert $x^B = 5^7$.

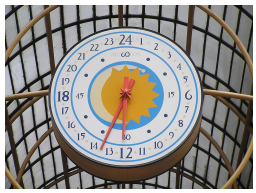
Der gemeinsame Schlüssel ist
$(x^A)^B = (x^B)^A = 5^{21} = 476837158203125$

Ungeeignet, denn

- leicht umkehrbar, und
- es treten zu große Zahlen auf.

$3 = \log_5(5^3)$

Beispiele für das Rechnen mit Resten



Uhrzeit.
Wie viel Uhr ist es in 25 Stunden? . . . in 100 Stunden? . . . in 1000 Stunden?

Wochentag. Welcher Wochentag ist heute in 1000 Tagen?

Teilbarkeit durch 9. Ist 123456789 durch 9 teilbar?

Bild: Wikipedia, CC BY-SA, Benutzer: Morio

Schreibweise

Definition

Seien x, n ganze Zahlen. Wir schreiben $x \mod n$ für den Rest, den x bei Division durch n lässt.

Beispiel

$36 \mod 31 = 5, \qquad 64 \mod 17 = 13, \qquad -4 \mod 17 = 13.$

Beispiel

$$\begin{aligned} 5^7 \mod 17 &= 5 \cdot (5^2)^3 \mod 17 = 5 \cdot (25)^3 \mod 17 \\ &= 5 \cdot 8^3 \mod 17 = 5 \cdot 8 \cdot 64 \mod 17 \\ &= 40 \cdot (-4) \mod 17 = -24 \mod 17 = 10 \end{aligned}$$

Zum Vergleich: $5^7 = 78125$.

Eine praktikable Version des Schlüsseltauschs

Öffentlich: (große Prim-)Zahl p, eine Zahl x, $1 < x < p$.

Alice

wählt eine Zahl $1 < A < p$ und schickt Bob die Zahl $x^A \mod p$.

Bob

wählt eine Zahl $1 < B < p$ und schickt Alice die Zahl $x^B \mod p$.

Alice und Bob können $x^{AB} = (x^B)^A = (x^A)^B \mod p$ berechnen und als gemeinsamen Schlüssel berechnen.

Schlüsseltausch, Beispiel

Öffentlich: (große Prim-)Zahl $p = 17$, eine Zahl $x = 5$, $1 < x < p$.

Alice

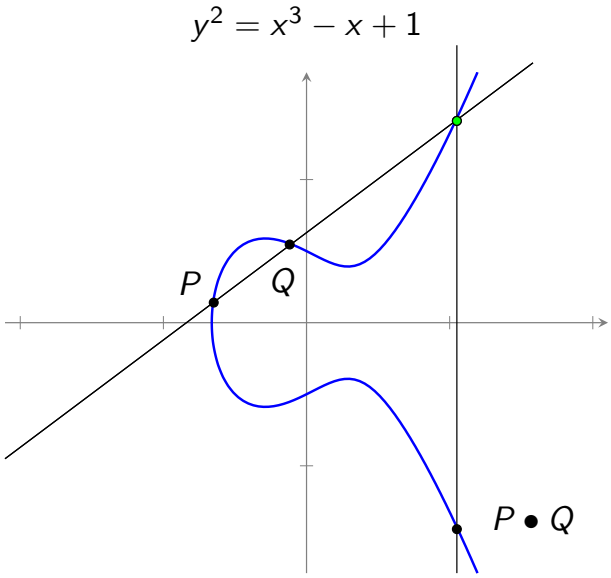
wählt die Zahl $A = 3$ und schickt Bob die Zahl $5^3 \mod 17 = 6$.

Bob

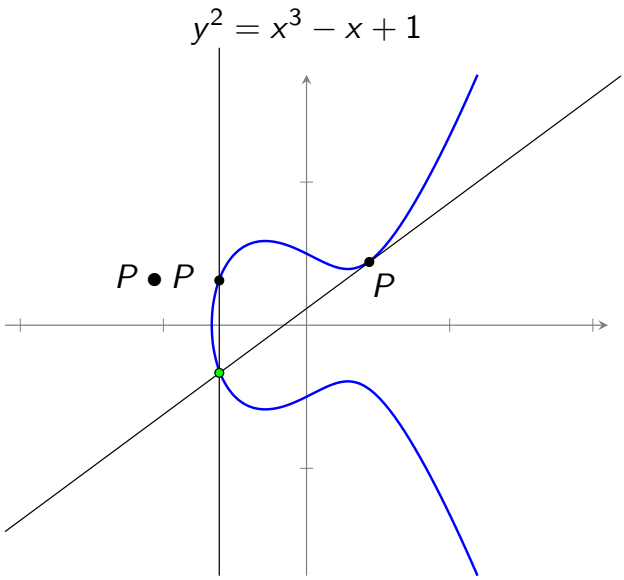
wählt die Zahl $B = 7$ und schickt Alice die Zahl $5^7 \mod 17 = 10$.

Alice und Bob können $5^{21} \mod 17 = 10^3 \mod 17 = 14$ berechnen und als gemeinsamen Schlüssel verwenden.

Kryptographie mit elliptischen Kurven



Kryptographie mit elliptischen Kurven



Diffie-Hellman-Schlüsseltausch mit Elliptischen Kurven

Öffentlich

Wähle eine elliptische Kurve und einen Punkt P darauf.

Alice

wählt eine Zahl A, berechnet $P^A = P \bullet \cdots \bullet P$ und schickt dies an Bob.

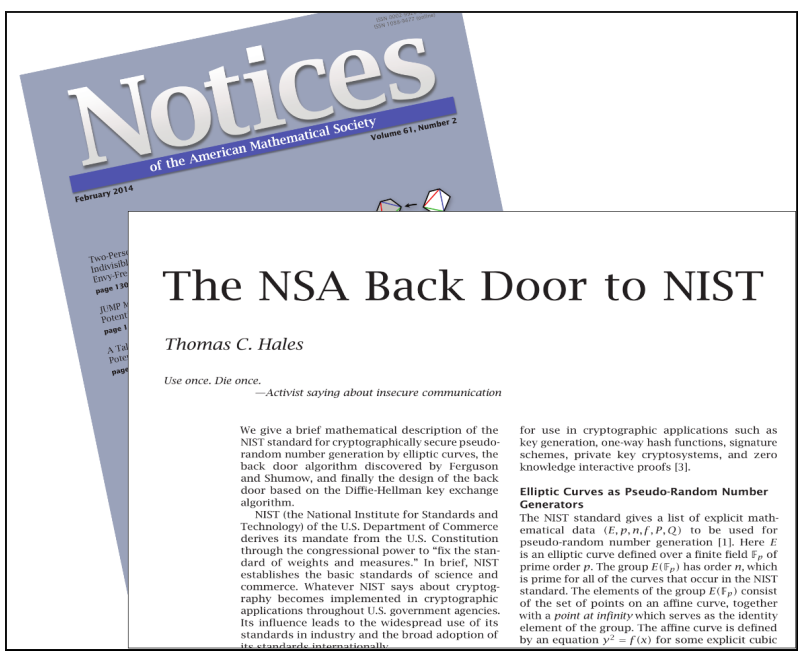
Bob

wählt eine Zahl B, berechnet $P^B = P \bullet \cdots \bullet P$ und schickt dies an Alice.

Gemeinsamer Schlüssel

die erste Koordinate des Punktes $(P^A)^B = (P^B)^A$.

Wie wählt man eine geeignete elliptische Kurve?



Quellen/Weiterführende Lektüre

S. Singh, *Geheime Botschaften*, dtv 2001.

`http://de.wikipedia.org/wiki/Kryptographie`

T. Körner, *The pleasures of counting*, Cambridge University Press, 1996.

J. Buchmann, *Einführung in die Kryptographie*, Springer-Verlag, 2010.

D. R. Stinson, *Cryptography – Theory and Practice*, CRC Press, 1995.

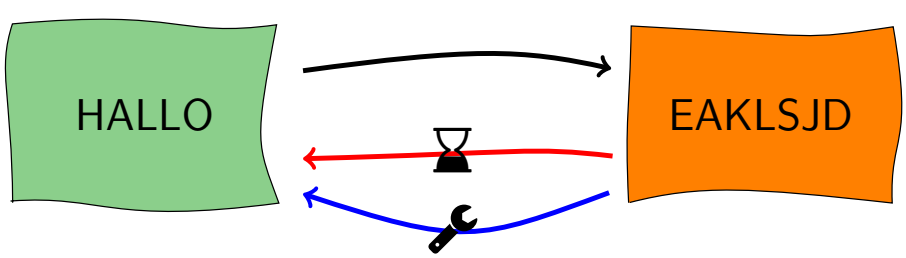
Prinzip der Public-Key-Kryptographie

Wir suchen eine "Maschine" (einen Algorithmus), die

(1) aus einem gegebenen Klartext schnell einen "verschlüsselten" Text berechnen kann,

(2) so dass sich aus dem verschlüsselten Text der Klartext *unter Zuhilfename zusätzlicher Informationen, die für (1) nicht benötigt werden,* schnell berechnen lässt,

(3) aber sich der Klartext ohne diese zusätzlichen Informationen nur mit erheblichem Aufwand aus dem verschlüsselten Text berechnen lässt.



Verschlüsselung mit RSA

Wähle große Primzahlen $p \neq q$, $N = pq$,
e teilerfremd zu $(p-1)(q-1)$.
Berechne f so dass $ef \equiv 1 \mod (p-1)(q-1)$.

K Klartext (als Zahl $< N$), C verschlüsselter Text.

Verschlüsselung

$C := K^e \mod N$

Entschlüsselung

Berechne $C^f = K^{ef} \equiv K \mod N$.

Der Satz von Euler

Satz

Seien p, q verschiedene Primzahlen.
Sei $N = pq$, $d \in \mathbb{Z}$ mit

$$d \equiv 1 \mod (p-1)(q-1).$$

Dann gilt $a^d \equiv a \mod N$.

Beispiel

$p = 5$, $q = 7$, $N = 35$, $d = 25$, $a = 3$.

$$3^{25} = 27^8 \cdot 3 \equiv (-8)^8 \cdot 3 \equiv (-6)^4 \cdot 3 \equiv 36^2 \cdot 3 \equiv 3 \mod 35$$

Entschlüsselung ohne Schlüssel?

Die einzige offensichtliche Möglichkeit, aus N, e und C wieder K zu berechnen, ist mit Hilfe von f. Aber f lässt sich nur dann aus e berechnen, wenn p und q bekannt sind.

Das Problem ist also, die Zahl N in ihre Primfaktoren zu zerlegen.

Dafür ist —bei entsprechender Größe von p und q— kein schnelles Verfahren bekannt. Primzahlen der entsprechenden Größe zu finden, ist vergleichsweise leicht. Eine übliche Größe für wichtige geheime Nachrichten wäre heutzutage, Primzahlen p und q mit ungefähr 300 Stellen zu verwenden.